CLAIMS

We claim:

1. A method affording privacy or anonymity on an Internet-type or other Communications medium, the method comprising:
   a) establishing a secure connection between a client and an intermediary site; and
   b) offering or providing one or more services through or on the intermediary site to the client.

2. A method as claimed in claim 1, wherein the services include using the intermediary site to forward communications between the client and destination sites so as to prevent one or more of the following:
   a) any logging of details of the true destination sites the client has visited by machines capable of monitoring client transactions by means of the secure client-intermediary connection;
   b) any logging of the contents of transactions between clients and destination sites by machines capable of monitoring client transactions by means of the secure client-intermediary connection;
   c) destination sites finding-out the true origin or location of clients by means of formatting client requests to giving the destination site the impression that the intermediary site was the origin of the communication.

3. A method as claimed in claim 1 or claim 2, wherein the services include one or more of the following:
   a) accessing of destination Internet sites by the client through the secure connection with the intermediary site and actively preventing any logging by Internet servers, providers, routers or other machines associated therewith that the destination sites have been visited by the client;
   b) sending or receiving e-mails while any logging of either the destination, source or contents of the e-mail is actively prevented;

c) storing files securely on the intermediary site;

d) transferring messages between multiple clients connected through the intermediary as in a secure telephone, conferencing, Internet "Chat", "Message Board" service or similar.

4. A method as claimed in any one of claims 1 to 3 and further comprising:

a) accessing of destination Internet or Internet-type service sites by the client through the secure connection with the intermediary site; and

b) actively preventing any logging by Internet servers, providers or other machines associated therewith that the destination sites have been visited by the client.

5. A method as claimed in any of the previous claims and further comprising:

a) establishing the secure connection between the client and the intermediary site;

b) allowing the client to use the secure connection to send a request to the intermediary site for forwarding to a destination site;

c) transforming the request into a standard request that can be interpreted by the destination site as originating at the intermediary;

d) sending the transformed client request from the intermediary to the destination site or a proxy for that site;

e) receiving the requested response from the destination site at the intermediary;

f) transforming the destination response into a response identified as being from the intermediary site; and

g) using the secure connection to return the response back to the original client.

6. A method as claimed in claim 5 and further comprising the step of transforming links and references in the response so that any future request made by the client based on the response from the destination site is made by the client through the intermediary site not directly to the destination site.

7. A method as claimed in any one of claims 1 to 6 and further comprising the intermediary site checking that a client connection remains open to the intermediary throughout a communication transaction so that destination responses can be delivered to the client and that the client is not attempting an anonymous denial of service attack on the destination site.

8. A method as claimed in any one of claims 1 to 5 and further comprising:
   a) sending or receiving e-mail by the client through the secure connection with the intermediary site; and
   b) actively preventing any logging by Internet servers, providers, routers or other machines associated therewith of details of the client, e-mail content, recipients and sender.

9. A method as claimed in any one of claims 1 to 5 and further comprising sending or retrieving a file by the client through the secure connection with the intermediary site and the intermediary site securely storing or retrieving the file.

10. A method as claimed in claim 9, wherein the intermediary site itself stores the file.

11. A method as claimed in any one of claims 1 to 10 and actively hindering Internet transaction sniffing.

12. A method as claimed in any one of claims 1 to 11, wherein the secure connection is an encrypted connection.

13. A method as claimed in claim 12, wherein the encrypted connection is an SSL connection.

14. A method as claimed in any one of claims 1 to 13 used to allow communication with destination sites where the client is restricted from directly accessing the

destination site by a restrictive Internet firewall, proxy server, physical limitations or other apparatus.

15. A method as claimed in any pervious claim comprising the intermediary listening for client requests on Internet port numbers above 1023.

16. A method as claimed in any one of claims 1 to 15 and adapted to improve the efficiency and speed of communication transactions by either:
    a) adding compression to the client-intermediary connection
    b) utilising a rapid communications channel between the client and the intermediary so as to reduce overall round-trip or delay times between the client and ultimate destination

17. A method substantially as herein described with reference to Figures 1 to 3 of the accompanying drawings.

18. Use of any of the methods of claims 1 to 17.

19. Apparatus configured to perform any one of the methods of claims 1 to 18.

20. Means to perform any of the methods of claims 1 to 18.